UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/027,714 | 12/21/2001 | David M. Austin | AUZ-002 P | 6090 |

21552 7590 12/24/2009
AUSTIN RAPP & HARDMAN
170 South Main Street, Suite 735
SALT LAKE CITY, UT 84101

| EXAMINER | |
|---|---|
| BROWN, CHRISTOPHER J | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2439 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 12/24/2009 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

usptocorrespondence@austin-rapp.com

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/027,714 | **Applicant(s)**<br>AUSTIN ET AL. | |
| | **Examiner**<br>CHRISTOPHER J. BROWN | **Art Unit**<br>2439 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *24 August 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Arguments*

Applicant argues that the claims do not teach countermeasure instructions that alter the operation of the observer program.

Examiner argues that Drake does teach countermeasures to an observer program, and Togawa in view of Drake teach the amendment including temporarily disabling, permanently disabling, and providing a decoy.

Although the examiner believes that it is well known to use a graphical user interface to control a security program (Windows, Macantosh), the examiner has included new reference Kim US 6,701,440 to advance prosecution. Kim teaches using a GUI with regard to security applications.

### *Double Patenting*

> The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-21 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-18 of copending Application No. 09/491,727. Although the conflicting claims are not identical, they are not patentably distinct from each other because It would have been obvious to one of ordinary skill in the art to store the second authentication value in a third file.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim(s) __1, 16, 17 ___ of application # 09/491,727 contain(s) elements of

Claim(s) ___1, 21___ of the instant application and as such anticipate(s) claim(s) _1, 21__ of the instant application.

All dependent claims are also anticipated by application # 09/491,727. These claims will be detailed in the final rejection.

## *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Togawa U.S. Patent No. 6,240,530, and further in view of Drake U.S. Patent No. 6,006,328 in view of Kim US 6,701,440.**

Togawa teaches a system for the detection and removal of computer malware.

Togawa fails to teach explicitly searching for observer programs as part of that malware.

Drake teaches security methods to protect against attacks by malicious software such as eavesdropping malware.

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the system of Drake with that of Togawa for the advantages of improved security by adding the features of protection against such malicious activities as eavesdropping to the ability of the scanning system as described by Togawa.

It is desirable within any computer system to maintain the security and integrity of such a system while preventing damage to the data and components included therein. Drake teaches protection of the client computer system against malicious software as does Togawa. Although each system teaches protection against a different type of malware by way of scanning the computer system, protecting against all forms of malware is desirable. (Drake Col 3 lines 30-52).

Regarding Claims 1 and 21: Observer program data characteristics descriptive of a plurality of observer programs where the observer programs are programmed to observe activities on a computer system and to create log data. (Togawa Fig 1 .sl, Col 5 lines 10-19 Drake Fig 4,5 Col 3 lines 31-52) As it is understood the detection of a virus and its type as within Togawa requires recognition of characteristics of a virus. Those characteristics residing within the computer systems various components as any particular virus infects that system; so then the same is true within the combined system for the detection of an observer program as defined by Drake. Obtain memory data of the computer by using computer instructions (Togawa Fig 1, Col 8 lines 14-30) As explained above the detection of the malware requires checking the system which is inclusive of the memory data; therefore in order for the functionality to proceed it must in some way obtain such data for scanning. It is well known to those of ordinary skill in the art that log data may contain screen shots, program usage, and websites visited, as admitted in the instant specification (page 2). Togawa teaches permanent disabling an intruder program through extermination (Col 8 lines 35-40)

Comparing memory data with observer program data characteristics for detection of an observer program (Col 8 lines 14-30) As it is known within the art virus scanning is the process of comparing two such sets of data. Further within the combined system the observer program characteristics are included within the set of the compared traits. Generating a result of whether an observer program is present (Fig 1, Fig 3-4 Col 5 lines 10-38) Detection denotes that a result is generated as to the response of the scanning process. Drake teaches temporarily disabling an observer program by making the rouge's task extremely difficult through encryption. (Col 6 lines 55-65). Drake teaches using decoy information to throw off an observer (Col 6 lines 54-57).

Kim teaches using a GUI to control the security applications taught by Kim (Col 11 lines 45-60). It is well known to those in the art to use a graphical user interface.
It would have been obvious to combine the GUI of Kim with the prior combination because a graphical user interface is easier to use than a text oriented interface.

Regarding Claims 2 and 3: Memory data includes startup and registry startup commands (Col 8 lines 14-30, Col 13 lines 19-56) As stated the memory contains all necessary information for the processes of the machine; these processes being inclusive of starting up necessary portions for operation thereof; such as the OS which includes a registry and the virus detection that being its own implementation scans the memory that these commands are located within.

Regarding Claims 4 and 5: Observer program characteristics include observer import/export table data for comparison with memory import/export table data to determine the presence of an observer program (Col 8 lines 14-30, Col 13 lines 19-56) As explained above all of the common features of the memory and functionality of the system are scanned via the anti-malware system.

Regarding Claim 6: Observer program characteristics include observer resource data for comparison with memory resource data to determine the presence of an observer program (Col 8 lines 14-30, Col 13 lines 19-56)

Regarding Claim 7: Observer program characteristics include observer file content data for comparison with memory file content data to determine the presence of an observer program (Col 8 lines 14-30, Col 13 lines 19-56) Additionally, as is shown and well known within the art file content is compared to malware characteristics for detection of such programs located commonly in such a place.

Regarding Claim 8: The comparing instruction compare the observer file content data with memory file content data at an offset address (Fig 1, Fig 3-4, Col 5 lines 10- 20, Col 13 lines 19-56) The process of scanning for malware is inclusive of the entire range of memory; therefore the process must offset the data being scanned by that which has already been.

Regarding Claim 9: The comparing instruction compare the observer file content data with a span of the memory file content data identified by an offset address (Fig 1, Fig 3-4, Col 5 lines 10-20, Col 13 lines 19-56) The process of scanning for malware is inclusive of the entire range of memory; therefore that which is scanned is a span of memory that is offset by the amount previously scanned.

Regarding Claim 10: Observer program characteristics include observer module loading data for comparison with memory module loading data to determine the presence of an observer program (Col 5 lines 10-20, Col 13 lines 19-56)

Regarding Claim 11: Observer program characteristics include OS observing functions for comparison with memory functions from the memory data to determine the presence of an observer program (Col 5 lines 10-20, Col 13 lines 19-56)

Regarding Claim 12: Memory data includes explorer extension data (Col 13 lines 19-56)

Regarding Claim 13: Memory data includes file use information (Col 13 lines 19- 56)

Regarding Claim 14: Memory data includes process information (Col 13 lines 19-56)

Regarding Claim 15: Memory data includes running process information (Col 13 lines 19-56)

Regarding Claim 16: Memory data includes loaded module information (Col 13 lines 19-56)

Regarding Claim 17: Memory data includes driver data (Col 13 lines 19-56)

Regarding Claim 18: Memory data includes kernel driver data (Col 13 lines 19- 56) All of the above stated separate memory data components are included within any resident memory of a common computer system that a system such as the combination of Togawa and Drake would be implemented upon.

Regarding Claims 19 and 20: Instruction to disable an observer program if present (Fig 1, Fig 10, Col 5 lines 10-50, Col 19 line 15 - Col 20 line 65)

Entering a startup command to load a kill program before the observer program is started (Fig 10, Col 19 line 15 - Col 20 line 65) As shown within the figure the system clears the memory then loads a secondary extermination routine, inclusive of the secondary OS and associated extermination routine, so that the observer program is not reloaded and instead the kill program is loaded and executed.

Rebooting the computer (Fig 1, Fig 10) As it is shown after the detection and initial clearing of memory the system must be rebooted with a separate non-infected operating system to further allow for the deletion of any other virus elements.

Starting the kill program by execution of the startup command (Fig 10, Col 19 line 15 - Col 20 line 65) As explained above the kill program is loaded at startup so the virus may not load.

Deleting the observer program startup command and files (Fig 10, Col 19 line 15 - Col 20 line 65) The process of clearing the memory as stated within the cited lines and exterminating the malware is the process of deleting the startup command.

## *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER J. BROWN whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571)272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher J Brown/ 12/17/09
Primary Examiner, Art Unit 2439